FEDERAL PKI POLICY AUTHORITY

September 11, 2012 MEETING MINUTES

USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:30 a.m. – 12:00 a.m. EST

9:30	**Welcome, Opening Remarks & Introductions**	**Mark Stepongzi, Chair (Proxy)**
9:35	**Discuss / Vote on August 2012 FPKIPA Minutes**	**Matt King**
9:40	**Criticality of FPKI Availability - Update**	**Toby Slusher**
9:50	**Discussion/Vote: USPS Cross-Certification Application**	**Matt King**
10:00	**FPKI Management Authority (FPKIMA) Report**	**Darlene Gore**
10:30	**FPKI Certificate Policy Working Group (CPWG) Report** **1. Discussion/Vote: PIV Content Signing Policy Change Proposal (Common CP)** **2. Other Updates**	**Charles Froehlich**
11:00	**SHA-1 Transition Status**	**SHA-1 Affiliates**
11:10	**VA Status Update**	**John Hancock / Eric Jurasas**
11:20	**FPKIPA Chair Update**	**Matt King**
11:30	**Other Agenda Items** o *If you cannot attend, please designate a proxy* o *Next FPKIPA meeting, October 16, 2012*	**Matt King**
12:00	**Adjourn Meeting**	**Mark Stepongzi (Chair Proxy)**

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	Mitchell, Debbie	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	T
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	P
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Rice, Barry	T
Department of Treasury (Treasury)	Wood, Dan	P
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	T
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb (Proxy to USPS)	A
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	T
United States Postal Service (USPS)	Stepongzi, Mark (Proxy for GSA)	P
United States Patent & Trademark Office (USPTO)	Kless, Patricia	T
Veterans Administration (VA)	Jurasas, Eric	T

b. Observers

Organization	Name	T – Telephone P – In Person A – Absent
Safer Institute	Boley, Ken	P
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
FPKIMA (Contractor, Protiviti)	Jarboe, Jeff	P
FPKIPA (Contractor, Protiviti)	Silver, Dave	T
CertiPath	Spencer, Judy	P
Identrust	Cox, Jerry	P
GSA FAS	Gore, Darlene	T
FPKIMA (Contractor, Protiviti)	DiDuro, John	P
DoD	Bures, Iva	T

B. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at USPS Headquarters, 475 L'Enfant Plaza, SW, Conference Room 4841, Washington, DC. Mr. Mark Stepongzi, Chair Proxy, called the meeting to order at 9:33 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

Discuss / Vote on August 14, 2012 FPKIPA Minutes, Matt King

There was a vote to approve the August 14, 2012 FPKIPA minutes. NRC motioned to approve; DOJ seconded. The motion was approved unanimously.

Approval Vote for August 14, 2012 FPKIPA Minutes			
Voting members	**Vote (NRC Motion; DOJ Seconded)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)	√		
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA) (Absent for vote)			√
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

Criticality of FPKI Availability - Update, Toby Slusher

Mr. Toby Slusher provided an update on the *Criticality of the FPKI Memo*. Revisions were made per the FPKIPA's direction at the last meeting. Additional comments were received since that last meeting. The FPKIPA agreed that a small group led by Mr. Slusher would streamline the memo to make it clearer and more to the point. The final version will be sent to Ms. Deb Gallagher for final review and submission to the CIO Council.

ACTION ITEMS:

1. Mr. Slusher will work to streamline, finalize, and submit the *Criticality of the FPKI Memo* to Ms. Gallagher for final review and submission to the CIO Council.

Discussion/Vote: USPS Cross-certification Application - Matt King

The USPS application for cross-certification with the FBCA was presented to the FPKIPA. Some discussion was held. USPS indicated they are working with other federal agencies to determine if USPS can meet those agencies' PIV-I needs. USPS is working to change the law limiting the digital services they can provide to citizens. USPS is currently immune from FISMA and HSPD-12 requirements because they are a Title 39 agency. USPS will cross-certify at Medium and Medium Hardware. They expect to have separate CA for Device certificates and will modify their application to reflect this plan. USPS plans to use one HSM for four CAs. Mr. Stepongzi provided additional information about the diagram USPS provided. It was agreed that the CPWG should update the *Crits and Methods* document with additional details about what is required in the architecture diagram. NRC motioned to approve; Treasury seconded. The motion was approved unanimously.

Approval Vote for USPS Cross-certification Application			
Voting members	**Vote (NRC Motion; Treasury Seconded)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)	√		
Drug Enforcement Administration (DEA CSOS)	√		

Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA)	√		
United States Postal Service (USPS)			√
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

FPKI Management Authority (FPKIMA) Report, Darlene Gore

Mr. John DiDuro presented a GFIRST Conference Trip report. The goal of attending the conference was to raise awareness of FPKIMA activity and enhance the relationship with US-CERT. As a result, the FPKIMA has been asked to participate in a US-CERT exercise. and the FPKIMA will work with US-CERT to incorporate PKI knowledge into US-CERT analyses. Ms. Wendy Brown presented additional information about recent cross-certifications and transition to new IP addresses, and noted that the next FPKI TWG will be on September 18th.

Sept2012 Slides for PA Meeting-final.pdf

ACTION ITEMS:

1. None.

FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

Mr. Charles Froehlich presented the CPWG Report.

a. Discussion/Vote: PIV Content Signing Policy Change Proposal

The PIV Content Signing change proposal is still under review. FIPS 201-2 requires the mediumDeviceHardware OID plus the PIV Content Signing EKU for certificates issued to Content Management Systems (CMSs). NIST has stated that they would reference a PIV Content Signing OID in FIPS 201 if it were included in the Common CP. The CPWG has recommended to NIST that FIPS 201-2 simply reference the Common CP for all PKI technical specifications. However, the PIV Content Signing Policy must be

defined in the Common CP in time for FIPS 201-2 to reference it. Adding this OID also provides an opportunity to ensure that Common Policy and PIV-I requirements are aligned and provides the opportunity to define narrower requirements for certificates issued to CMSs that are used to sign the content on the card.

Both DoD and NIST have raised questions, and although the number of affected CMSs is small, SSPs need to provide input to this proposal regarding cost and the length of transition time. Lastly, the certificate profiles will need to be updated if this change proposal is approved.

b. Other Updates

CPWG review of the DoD cross-certification mapping is in progress. The CPWG will begin review of the ExoStar cross-certification mapping. The USPS mapping will be reviewed after the Exostar mapping.

CertiPath raised a question about standards for issuing PIV-I credentials to non-U.S. persons, in non-U.S. locations, by non-U.S. providers, that may or may not be used for access to U.S. facilities and systems. Ms. Judy Spencer is preparing an expanded white paper on this subject. DigiCert has raised similar questions, as well as questions about what documentation is acceptable for proving the identity of non-U.S. persons outside the U.S. Customs and Immigration Service (USCIS) I-9 Form parameters. Discussions are continuing on this subject.

PIV-I Card Re-testing requirements have been reviewed and are nearing finalization, but additional provider input is still required.

Change Proposals to both the FBCA and Common CPs regarding broadening implementation of digital signatures for PKI transaction have been developed and will be discussed at the next CPWG meeting—agenda permitting.

Discussion of the need for, and content of, a change proposal to address CRL publication for CAs that retire a private key but are not terminating service, will also be held at the next opportunity.

Mr. Dan Wood mentioned that SWIFT is interested in cross-certifying with the FBCA and was looking for guidance on the process. Ms. Judy Spencer offered to provide insight. Mr. Wood stated that he would provide contact information as appropriate.

SHA-1 Transition Status, SHA-1 Affiliates

Mr. Matt King asked for updates related to Affiliate transition from SHA-1. DEA is moving forward with their transition. VeriSign still has customers (e.g., NRC and at least one other agency) that need to transition to SHA-2. SAFE had planned to transition in June 2012, but some customers were not ready so their transition has been delayed. Symantec/VeriSign already has several SHA-2 CAs; they just need to transition their customers still using SHA-1. CertiPath is running a SHA-2 CA, but is still

on the SHA1 FRCA to support its members who only support SHA-1 due to their requirement to interface with DoD. Their transition is largely dependent on DoD's plans to fully transition to SHA-2. Illinois was not present to provide an update.

ACTION ITEMS: None

VA Status Update, John Hancock / John Hancock, Eric Jurasas

Mr. Eric Jurasas will coordinate with Mr. King to ensure the FPKIPA has the right point of contact information to obtain the most recent status updates on VA's progress toward addressing issues identified in the OIG Report. No update was available.

ACTION ITEMS: None

FPKIPA Chair Update, Matt King

Mr. King presented the FPKIPA Chair report and provided status of change proposals, documents, and cross-certifications.

FPKIPA Chair Report_11SEP12_fina

Upcoming meetings and events:

Meeting	Date
Strong Logical Access Tiger Team (SLATT)	**Wednesdays 10:00 – 11:00am**
ISIMSC	**September 17, 2012**
CPWG	**September 18, 2012**
IAB	**September 26, 2012**
ICAMSC	**September 26, 2012**
TWG	**September 18, 2012**

The next FPKIPA meeting is October 16, 2012. The meeting will be at USPS.

Adjourn Meeting

Mr. Stepongzi adjourned the meeting at 11:24 a.m. EST.

FPKIMA Open Action Items

Number	Action Statement	POC	Start Date	Target Date	Status
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	12-Jul-11	13-Sep-11	Open
460	The FPKIMA will work with Mozilla to determine what Mozilla will accept if we do not provide CPSs	Wendy Brown	8-May-12	30-Jul-12	Closed
464	Ms. Darlene Gore to provide the briefing that was given to the BOAC to Mr. Jeff Jarboe for distribution to the FPKIPA.	Darlene Gore, Jeff Jarboe	10-Jul-12	17-Jul-12	Closed
466	Ms. Gallagher to forward complaints about some agencies not accepting external PIV-I and SHA-1 credentials to Ms. Deb Mitchell.	Deb Gallagher	10-Jul-12	17-Jul-12	Open
467	Mr. Slusher will draft language with Mr. Froehlich, Mr. King, and Mr. Silver, to add language about PKI uses and business processes to the FPKI Criticality letter and send the final version to Ms. Gallagher.	Toby Slusher	14-Aug-12	11-Sep-12	Closed
468	Ms. Gallagher will submit the final FPKI Criticality Letter to the ICAMSC.	Deb Gallagher	14-Aug-12	30-Sep-12	Open
469	The FPKIMA will send information to the FPKIPA mail list about how to participate in the Mozilla discussion.	Wendy Brown	14-Aug-12	11-Sep-12	Closed
470	Mr. Froehlich will lead CPWG discussions to develop a change proposal to add language to the FBCA and Common policies that requires digital signature of supporting documents	Charles Froehlich	14-Aug-12	11-Sep-12	Open
471	The CPWG will review the Common Policy to determine if another change proposal is required to allow for the long-term CRL issued by the Legacy Common Policy CA	Charles Froehlich	14-Aug-12	11-Sep-12	Open
472	Mr. Froehlich will lead discussions in the CPWG to develop a PIV Content Signing change proposal.	Charles Froehlich	14-Aug-12	11-Sep-12	Open

Number	Action Statement	POC	Start Date	Target Date	Status
473	Any Affiliate still cross-certified with the SHA1 FRCA needs to begin providing updates on their plans to transition off the SHA1 FRCA prior to December 31, 2013. This includes: DoD, DEA, Illinois, Symantec, CertiPath, and SAFE.	FPKI Affiliates	14-Aug-12	11-Sep-12	Open
474	Mr. Jason Miller will work to obtain more detailed information on the VA remediation efforts.	Jason Miller	14-Aug-12	11-Sep-12	Open
475	Ms. Gallagher will resubmit the metrics related to the FPKI Security Profile to the FISMA team	Deb Gallagher	14-Aug-12	11-Sep-12	Open